Section 1: GENERAL PRIVACY RULES

1.5 Privacy Safeguards

POLICY

1. Commitment:
    a. The University of Florida (UF) is committed to safeguarding the confidentiality and security of Restricted Information created, received, stored, or transmitted by UF so that it is only used or disclosed in accordance with UF's policies and federal and state regulations.
    b. UF develops, implements, and maintains reasonable and appropriate administrative, technical, and physical safeguards to preserve the privacy and security of restricted data it creates, receives, stores, and transmits.
    c. Every person at UF with access to Restricted Information in any format, including without limitation, paper, electronic, graphic, video, oral/sign language, or any other format, is responsible for safeguarding its confidentiality and security, and for complying with all information privacy and security policies and procedures approved by UF.
    d. All Protected Health Information (PHI) and other restricted data, created, received, maintained, and transmitted by UF in all formats, must be secured from unauthorized access at all times, to protect the information from damage, loss, alteration, tampering, and fraudulent use.
    e. UF established a university-wide “clean desk program” to standardize and enhance the safeguarding of information across the university. A clean desk policy is an important tool to ensure that all Restricted and/or Sensitive Information is properly secured and or removed from a workspace when the information is not in use or an employee leaves his/her workstation. A clean desk policy is also consistent with NIST standards and part of basic privacy controls.
2. Application:
    a. UF places significant trust in all who have access to restricted data and, with that trust, comes a high level of responsibility.
    b. Uses and disclosures of restricted data for any purposes other than those authorized constitute privacy violations.
    c. Deliberate disregard of this policy or the safeguards created to implement this policy may result in disciplinary action up to and including termination of employment and/or expulsion from academic programs by UF.
3. Access to electronic PHI: is defined by levels based on users’ roles and responsibilities.
    a. Workforce: Health-related colleges, departments, and clinics must define and justify levels of access to PHI for their workforce members relative to their assigned duties and professional “Need to Know”.
    b. Students: The Privacy Office, working with the health-related colleges, defines the levels of access to PHI for students and other trainees who require such access for the completion of academic studies.
4. Computer Surveillance: UF and UF Health Shands (Shands) have the capability to track and log access and activities in much of its information and computing environment. All user activity on UF Health Science

Center (HSC) Information and Computing Environment components, including, but not limited to, access through personal computing devices, is subject to review.

5. Use of Interpreters: The patient's authorization is not required for use of an interpreter if the patient speaks a language other than English or is hearing impaired, and the provider uses the interpreter to communicate about treatment, payment or health care operations. The following conditions apply:

    a. UF may use an organization or individual as a business associate to perform interpreter services on its behalf, including private commercial companies, community-based organizations, or telephone interpreter service lines. A valid Business Associate Agreement is required.

    b. UF may use a member of UF's workforce (i.e., a bilingual employee, a contract interpreter on staff, or a volunteer), as long as the employee has completed HIPAA training and signed a Confidentiality Statement and the patient agrees to the arrangement.

    c. UF may communicate with a patient through the patient's family member, close friend, or other person identified or approved by the patient to serve as his or her interpreter for a healthcare encounter. That interpreter is not considered a business associate of the health care provider.

    d. The health care provider may obtain the patient's agreement to the use of an interpreter either in writing or verbally, or the provider may reasonably infer, based on professional judgment and the circumstances, that the patient does not object to the disclosure of PHI to the interpreter.

    e. Video- and Audio-Conferences: The following items must be defined and approved prior to initiating electronic conferencing systems:

        i. Security of transmissions, including adequacy of privacy and security at both the point of initiation and point of reception, transmission modes, and network security.

        ii. Compliance with interstate and international privacy laws, as appropriate.

        iii. Initiation of a Business Associate Agreement with any service provider, as appropriate.

    f. Personal Communications: Video- and audio- conferencing as described in this policy are not intended to include communications between patients and providers (or subjects and researchers) using a personal account on a commercial Internet telephony service with or without a video component (i.e., Skype, Google Talk, Yahoo! Messenger, Facebook Video, etc.). However, these types of communication also require that the patient be directed to review the Alert for Electronic Communications and sign an authorization for use and disclosure of PHI.

6. Use of Telecommunication Devices for the Hearing Impaired

    a. Telecommunications Relay Services (TRS): The TRS is a public service, available without cost to all persons and businesses, none of whom need to employ, contract with or otherwise establish business relationships with the TRS. When performing services for a covered entity (CE), the TRS is not acting for or on behalf of the CE and is not the CE's business associate.

    b. When a covered health care provider initiates a call using the TRS without the individual's prior agreement, the individual must be given an opportunity to agree or object to disclosures of PHI to a TRS Call Assistant so that pertinent information can be shared during the telephone communication. (See 45 CFR §164.510(b))

DEFINITIONS:

1. ***Authentication:*** the corroboration that a person is the one claimed.

2. *Information system:* an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.
3. *Integrity:* the property that data or information have not been altered or destroyed in an unauthorized manner.
4. *Interpreter:* One who translates from one language into another, usually orally, but also by hand-signs.
5. *Safeguards*: Rules and specific methods established to protect restricted data from unauthorized access, accidental or intentional use, disclosure, transmission, or alteration, and inadvertent or incidental disclosure to unintended recipients.
6. *Sign Language:* A formal or informal system of manual, facial, and other body movements as the means of communication, especially among deaf people.

REQUIREMENTS

1. Security standards – General rules: Covered entities and business associates must do the following:
    a. Ensure the confidentiality, integrity, and availability of all electronic PHI the covered entity (CE) or business associate creates, receives, maintains, or transmits.
    b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
    c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule.
    d. Ensure compliance with the HIPAA Privacy and Security Rules by its workforce.
2. Implementing Safeguards: A CE or business associate must comply with the applicable standards as provided in the HIPAA Security Rule with respect to all electronic PHI.
3. Information access management: Implement policies and procedures for authorizing access to electronic PHI that are consistent with the applicable requirements of the HIPAA Security Rule.
4. Family Members and Friends: A CE may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care. See also policy 3.3 Uses & Disclosure of PHI: Patient's Family Members & Friends.
5. Minimum necessary applies: When using or disclosing PHI, a CE or business associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure.

PROCEDURES

1. Clean Desk Program
    a. The purpose for this policy is to establish the *minimum requirements* for maintaining a "clean desk" – where Restricted or Sensitive information about our students, faculty, staff, or patients, and our intellectual property and research data remains secure.
    b. Physical Controls
        i. Employees are required to ensure that all Restricted or Sensitive information, hardcopy or electronic, is properly secured when not in use, at the end of the workday or when they are

expected to be gone for an extended period. Examples of additional controls are provided below.

- Place paper records in protective covers whenever possible.
- Printouts containing Restricted or Sensitive information should be immediately retrieved from a printer.
- Keep records and documents that contain Restricted or Sensitive information that are not currently in use in locked drawers, cabinets, or occupied by authorized personnel at all times.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

ii. Document and Device Destruction

- Shred discarded records after their minimum retention requirement (or immediately if the record is a working document) and shortly after they are no longer needed. Please refer to Record Retention Schedules published by UF Records Management.
- Maintaining personal destruction bins is permitted if the bin is properly marked (i.e. "for secure destruction" or "shred only"), maintained in a secure area, and emptied daily.
- Do not place papers containing PHI or other Restricted Data in open waste receptacles.
- Ensure Proper Disposal of Devices: Contact the UF Information Security Office or place an IT Service Request to prepare mobile computing and storage devices for disposal in compliance with Information Security Reuse and Disposal Standards.

iii. Computer Workstations

- To prevent unauthorized use or disclosure, place computers, monitors, and similar data storage and display devices in areas that limit viewing and prevent access by unauthorized persons; position electronic displays away from public view or shield the viewing screen.
- Computer workstations must be locked when workspace is unoccupied.
- Laptops and portable devices must be either locked with a locking cable or locked away in a drawer if the device remains in an unsecured area.

iv. Place computer printers, copiers, and fax machines in locations that can either be locked when not occupied or that are staffed by authorized personnel at all times.

2. Administrative Safeguards

a. Policies and Procedures: Follow the policies and procedures for preventing, detecting, containing, and correcting information security breaches and violations, as required by Information Security personnel.

b. Incident Management: Report security incidents involving inappropriate use or disclosure of PHI to the Privacy Office immediately.

i. Report known and suspected security incidents to the appropriate Information Security Officer for investigation, repair, restoration, and disciplinary action, as necessary.

ii. Security incidents include hoax e-mails, hacking, altered data, deliberate disruptions of service, viruses, worms, and other unauthorized use of computer accounts and systems.

c. Termination: When an employee terminates employment, collect keys and other access devices if the employee's job duties included authorized access to any area where PHI is stored or used. Please refer to the UF HR Employee Exit Checklist for details.

d. Required Training: All workforce members in UF's health care components complete privacy and security training at orientation and annually.

3. Technical Safeguards:

   a. Access Controls and Passwords:

      i. To prevent unauthorized use, program all electronic devices with log-on processes, activate screen-savers that turn on automatically and use strong passwords.

      ii. Do not write down, post, include in e-mail, or otherwise share passwords with anyone.

      iii. Do not bypass password entries by auto-logons or "save password" options.

   b. Encrypt all PHI stored on removable electronic storage media (cards, CD's, flash devices, etc.).

   c. Access to PHI:

      i. Address requests for access to PHI to the appropriate Identity & Access Administrator, records custodian, or information systems coordinator according to where the PHI is stored. Provide required documentation as necessary to justify the request for access.

      ii. For Employees:

         - Epic Electronic Health Record Access: Route all employee (UF or Shands) requests for access to the current electronic medical record (EHR) system and other UF or Shands health-related computer systems to UFHS Identity and Access Management.

         - Axium Electronic Dental Record Access: Route all employee requests for access to the current electronic dental record system to the UF College of Dentistry IT System Administrator.

      iii. For Students: Colleges and other units requesting access to the current (EHR) system for their students should direct the requests to the UF Privacy Office for review and approval.

         - If the student needs access to medical records for a class and will receive some form of academic credit for the work, see also 6.4: Student Data Access Policy.

         - If the student is employed and needs access to medical records for assigned job duties, follow the procedure above for employees.

   d. Terminating Access to PHI:

      i. Managers, supervisors, and proctors:

         - Monitor needs for access to PHI in all formats by workforce members so that access is not continued beyond the actual need.

         - Notify Identity and Access Management immediately when an employee terminates employment so that access to electronic data systems is terminated.

      ii. Account managers: Terminate access to electronic PHI when the employment of, or other arrangement with, a workforce member ends or as required by applicable UF policies.

   e. Verbal Communications in Healthcare Areas

i. Speak quietly when discussing a patient's PHI and avoid the use of patients' names or other identifiers in conversations whenever possible.

ii. Do not discuss PHI in public areas, either verbally or by sign-language; move to private areas for exchange of private information.

iii. Conduct telephone conversations that include PHI in private areas, if possible.

iv. Make reasonable efforts to verify the identity of the other person(s) before proceeding with a telephone conversation, using departmental procedures or the verification guidelines or Policy 3.9: Verification of Identity and Authority of Personal Representatives.

v. Answering Machines:

- Do not leave detailed PHI in a message (diagnoses, lab test names or lab results, surgical procedures, etc.) or with an unknown person who takes a message for a patient.
- When leaving a message is necessary and appropriate, provide minimally necessary information to be useful to the patient, such as your name and callback number, a generic location similar to "University of Florida Physicians Clinic," and the purpose of the call, such as changed appointment, insurance questions, etc. Areas that provide certain types of healthcare services may adopt more restrictive practices.

REFERENCES

1. HIPAA Security Rule, 45 CFR Parts 160 and 164 (Subparts A and C).
2. National Institute of Standards and Technology. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations* (SP 800-53)
3. UF Information Technology Acceptable Use Policy and Information Security policies available at, https://it.ufl.edu/policies/.

EXHIBITS

None